Achieving a Sustainable Cybersecurity Strategy

*Sustaining a strong cybersecurity stance is more difficult as the threat environment expands and cyberattacks become more virulent. **Carolyn Duby,** field CTO for Cloudera, discusses tactics — including greater collaboration between state and local governments — to maximize protection.*

How have the pandemic and other disruptors impacted cybersecurity risk in the past two years?

The pandemic accelerated trends that were already in motion. Digital innovation increased to meet the need for digital interactions when face-to-face interactions weren't possible. In addition, the massive shift to working from home impacted risk. When the pandemic hit, most organizations didn't have all the policies, procedures and tools in place to effectively secure those environments. Another disruptor is the changing geopolitical landscape. Cyber warfare is becoming a mainstream weapon for many nation states. And then there is the explosion of fraud as a service. Attackers are taking advantage of the fact that organizations' defenses are not ready for remote work and these other changes.

What should organizations consider as they address security from the edge to the core?

With trends like 5G, bring your own device and the proliferation of IoT, the threat landscape is much bigger than before, and it's easier for attackers to exploit because so many devices are poorly secured. Organizations must think strategically about the assets they have, their value to an attacker, how they could be exploited and how they can be protected. Organizations also need to consider how they would respond to a cyber incident. Many local governments don't have the resources to successfully address these issues on their own. Having a state-level response to help investigate and remediate an incident is increasingly important.

How can AI and machine learning (ML) help strengthen cybersecurity, fraud protection and compliance?

There's a lot of potential for AI and ML to improve detection and response. These technologies can help organizations find anomalies that may indicate a security threat, investigate security alerts and reduce the number of alerts they recieve. The strength of AI and ML is that they can adapt to changes within the environment. They also act as force multipliers. The volume of security alerts and information coming from networks is more than any human could possibly track. AI and ML augment the human workforce.

What platform capabilities are important for enabling AI, endpoint protection and other security capabilities?

First, you need to access data in a consistent, open format and in a secure, governed way so you can use the data to train AI models. Second, you need to retain a long historical context to train AI algorithms — so you need a platform that can scale to handle the storage, analysis and processing that goes behind that. Third, comprehensive information about your network — including cloud environments and endpoints — must be in one place, so you have a complete understanding of all the pieces and what's happening across the network.

How can organizations better leverage their existing cybersecurity investments?

Leveraging existing investments well is really about investing in your team. Organizations must make sure staff members can effectively use the security tools that are in place. A lot of breaches and incidents happen because the team lacks training. Teams also need a unified environment for all those different tools, so information is in one place and they can easily correlate it. It's a combination of people, processes and tools, and then bringing them all together to constantly improve.

State and local governments increasingly share services and resources with other entities. What should they keep in mind?

It's a matter of examining how their relationships with others can be exploited, and then reducing that risk. Third parties can be used as an attack vector. So, agencies should always examine what data and other resources they're sharing with outside organizations. Constantly evaluate those relationships — as well as the third party's relationships with others — and ask whether it's necessary to share data with that entity. When sharing is necessary, ensure third parties are protecting your data in the best way possible.

Learn more at **Carah.io/GT-Dec-Cloudera**

I DISCOVERED
how to prevent maintenance problems
from becoming safety problems.

It’s not your data. It’s how you use it. Whether pushing the envelope of aerospace design or delivering vaccines years ahead of schedule, harnessing data to transform your business requires the power of artificial intelligence and machine learning to translate complex sets of information into clear and actionable insights. Cloudera’s enterprise data cloud platform accelerates data analytics at every stage of the data lifecycle, with security and governance built in, to make your hybrid cloud move your business.

Learn more at **cloudera.com/datamovesyou**

CLOUD=RA
Data That Moves You

#cloudera.com/publicsector